
UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

| | | |
|--------------------------|---|------------------------------|
| UNITED STATES OF AMERICA | : | Mag. No. 17-5016 (TJB) |
| | : | |
| v. | : | Hon. Tonianne J. Bongiovanni |
| | : | |
| JIAN YANG ZHANG, | : | |
| a/k/a "KEVIN ZHANG" | : | CRIMINAL COMPLAINT |

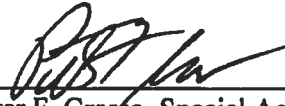
I, Peter F. Grasso, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.



Peter F. Grasso, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
September 15, 2017 at Trenton, New Jersey



HONORABLE TONIANNE J. BONGIOVANNI
UNITED STATES MAGISTRATE JUDGE

RECEIVED
SEP 15 2017
AT 8:30
WILLIAM T. WALSH
CLERK

ATTACHMENT A

COUNT 1

(Unauthorized Access of a Protected Computer)

On or about October 28, 2015, in the District of New Jersey, and elsewhere, defendant

JIAN YANG ZHANG, a/k/a "KEVIN ZHANG"

intentionally accessed a computer without authorization and exceeded authorized access to a computer, and thereby obtained information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain,

In violation of Title 18, United States Code, Section 1030(a)(2) and (c)(2)(B)(i).

COUNT 2

(Interception of Electronic Communications)

From on or about August 13, 2015 to on or about February 2, 2016, in the District of New Jersey, and elsewhere, defendant

JIAN YANG ZHANG, a/k/a "KEVIN ZHANG"

intentionally intercepted and endeavored to intercept electronic communications, as defined in Title 18, United States Code, Section 2510(12), to wit, incoming email messages sent to the email accounts of Company 1 employees.

In violation of Title 18, United States Code, Section 2511(1)(a).

ATTACHMENT B

I, Peter F. Grasso, am a Special Agent with the Federal Bureau of Investigation (“FBI”). I have knowledge of the facts set forth below as a result of my participation in this investigation as well as from my review of reports from, and discussions with, other law enforcement personnel. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

1. At all times relevant to this Complaint:

a. Company 1 was a New Jersey based importer and wholesaler of general merchandise that supplied products to dollar stores, discount stores, and wholesalers across the United States.

b. Company 1 was created in 2013 by owners M.M., A.I., F.I., defendant JIAN YANG ZHANG, a/k/a “Kevin Zhang” (hereinafter “ZHANG”), and various Zhang family members (collectively and with Zhang, the “Zhang Family”). The Zhang Family has other family members, property and business interests in China.

c. Company 1 maintained a website at the domain name [Company 1].com. In registering this domain, ZHANG listed himself as the registrant, with an address in Whitestone, New York (the “Whitestone, NY Address”)¹ and email address kevin@[Email 1].com, and as the domain administrator, with the Whitestone NY Address and email address jz118@[Provider A].com.

d. Company 1 maintained email accounts for its owners and employees using an email server provided by Provider B. For example, while working at Company 1, ZHANG used a Company 1 email address of kevin@[Company 1].com. ZHANG served as the email administrator for Company 1 from 2013 until his departure from Company 1 in February 2015.

e. Direct Containers Inc. was a New York corporation that did business in New Jersey, including, but not limited to, importing shipping containers to New Jersey. Direct Containers Inc. was established by the Zhang Family in May 2011.

2. In mid-2014, M.M., A.I., and F.I. had a dispute with the Zhang Family. As a result of this dispute, between October and December 2014, the parties negotiated a number of agreements that ultimately resulted in M.M., A.I., and F.I. buying out the Company 1 interests owned by the Zhang Family. As part of the transaction, the Zhang Family agreed to a restrictive covenant that precluded them, with limited exceptions, from importing or selling goods in North America or the Caribbean for a period of three years. The Zhang Family further agreed that

¹ According to AT&T records, Zhang owns a cellular telephone subscribed to him in his name at the Whitestone, NY Address.

their company, Direct Containers Inc., would act as Company 1's exclusive supplier of wholesale goods purchased from China.

3. In the midst of these buyout negotiations, on October 30, 2014, unbeknownst to M.M., A.I., and F.I., ZHANG created a hidden sub user account named "[Company 1]_admin" (hereinafter, the "Admin Account") within the Company 1 email server account. According to Provider B records, ZHANG initially registered the hidden Admin Account under the name "kevin" with a contact email address of kevin@[Company 1].com. ZHANG subsequently changed the name from "kevin" to "Admin" and deleted the contact email address.

4. In December 2014, the parties executed a Membership Transfer Agreement, pursuant to which the Zhang Family agreed to sell their membership interests in Company 1 to the remaining owners for approximately \$2,750,000.² Under that agreement, the Zhang Family agreed to return to the remaining owners "all of the property of [Company 1] in their possession to include the email server, along with all passwords and other credentials necessary to operate, manage and administrate [Company 1's] email, servers and network."

5. ZHANG was officially separated from Company 1 on December 14, 2014 but stayed on as the email administrator for approximately two months to help with the transition. When ZHANG left in February 2015, he provided F.I. with the credentials to log into the email server, but did not disclose that he had created the Admin Account. F.I. then logged into the email server and changed the password provided by ZHANG.

6. Despite having turned over the login credentials, ZHANG continued to access the Company 1 email server without authorization by using the hidden Admin Account. For example, ZHANG logged into the Company 1 server on, *inter alia*, the following occasions and conducted the following actions:³

a. On August 12, 2015, ZHANG changed the password for the Postmaster Mailbox (postmaster@[Company 1].com), an email account that was created automatically when Company 1 opened its account and set up its server with Provider B.

b. On August 13, 2015, ZHANG set the Postmaster Mailbox to forward all email communications sent to that account to dsf@[Provider A].com. Approximately two minutes later, ZHANG reset the Postmaster Mailbox to forward all email communications sent to that account to tonydisano123@[Provider C].com, and set the email mailboxes for F.I., M.M., and J.S. (a Company 1 logistics employee) to forward copies of all email communications sent to those accounts to the Postmaster Mailbox.

c. On August 29, 2015, ZHANG enabled spam folders for F.I., J.S., and M.M.'s email accounts, and set filters for email communications from one of Company 1's

² Per the Zhang Family's instructions, the consideration for the deal, structured as a series of payments over time, was to be wired to the Zhang Family's bank accounts in China.

³ According to Provider B records, between October 30, 2014 and December 22, 2015, the Admin Account was logged into approximately 33 times from various IP addresses.

suppliers so that such email communications would be sent to the spam folders and, thus, not visible in F.I., J.S. and M.M.'s email inboxes.

d. On September 23, 2015, ZHANG set the email mailboxes for F.I. and J.S. to forward copies of all email communications sent to those accounts to the Postmaster Mailbox and set the Postmaster Mailbox to forward all email communications sent to that account to mikedisano123@[Provider C].com.

e. On October 28, 2015, ZHANG set the email mailboxes for F.I., A.I., M.M., J.S., and K.S. (the Company 1 internal accountant) to forward copies of all email communications sent to those accounts to the Postmaster Mailbox, and set the Postmaster Mailbox to forward all email communications sent to that account to kenjohnson909@[Provider C].com.

f. On December 18, 2015, ZHANG set the Postmaster Mailbox to forward all email communications sent to that account to john8545@tech-center.com, and set the email mailboxes for F.I., K.S., M.M., and J.S. to forward copies of all email communications sent to those accounts to the Postmaster Mailbox.

7. Several of the IP addresses used during these and other Admin Account logins are connected to ZHANG.

a. For example, the password update described above in paragraph 6a was performed on August 12, 2015 by a user logged into the Admin Account from IP address 1 ("IP 1"). According to Verizon records, from March 2015 through February 2016, IP 1 was assigned to a Zhang Family member at the Whitestone, NY Address. Additionally, per Provider A records, IP 1 was used to log into the jz118@[Provider A].com email account on numerous dates from March 2015 through February 2016. Additionally, according to Provider A subscriber records, the subscriber for jz118@[Provider A].com was "Mr kevin Zhang" with several alternate email addresses, including kevin@[Email 1].com and kevin@[Company 1].com.

b. As another example, the email forwarding described above in paragraph 6e was set up on October 28, 2015 at approximately 3:16 A.M. (EDT) by a user logged into the Admin Account from IP address 2 ("IP 2"). Approximately six minutes earlier, at 3:10 A.M. (EDT) on the same day, a user logged into the jz118@[Provider A].com email account from IP 2.

8. Moreover, ZHANG is connected to the creation of the tonydisano123@[Provider C].com account discussed above in paragraph 6b. Specifically, that email account was created on August 13, 2015, approximately 13 minutes (EDT) before the email forwarding was set up, by a user who was logged into gmail from IP address 3 ("IP 3"). IP 3 was assigned to SLK Cellular, 11-402 15th Ave., College Point, NY, which is a corporate entity that was collocated with Direct Containers Inc. (the Zhang Family's company).

9. Additionally, on December 29, 2015, K.S. (the Company 1 internal accountant), acting at the direction of M.M., sent M.M. a ruse email stating that Company 1 had received a

letter from the Internal Revenue Service (“IRS”) addressed to ZHANG. In reality, Company 1 had received no such mailing. On January 4, 2016, ZHANG sent an email to F.I., A.I., M.M., and K.S. stating that he was expecting mail from the IRS and inquiring whether they had received any letters. Thus, ZHANG presumably learned of the purported IRS mailing through his unlawful interception of Company 1 employees’ email, which he had set up through an unlawful intrusion of the Company 1 email server.

10. The wire communications that ZHANG intercepted included, *inter alia*, confidential emails from Company 1’s customers and suppliers. Access to these emails provided ZHANG and Direct Containers Inc. with a competitive advantage in the marketplace, and caused Company 1 to suffer significant losses and damages.